NAVAL WAR COLLEGE
Newport, R.I.

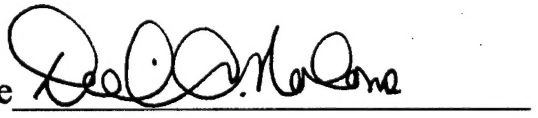
"Targeting Command and Control Warfare as Operational Fires."

By

Daniel A. Nolan III
Lieutenant Colonel, U.S. Army

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Joint Military Operations Department.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature 

17 May, 1998

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	**7. Address:** NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): (Unclassified) Targeting Command and Control Warfare as Operational Fires.	
9. Personal Authors: LTC Daniel A. Nolan III, USA	
10.Type of Report: FINAL	**11. Date of Report:** 18 May 1998
12.Page Count: 16	
13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: C2W, Information, Warfare, Operations, Targeting, Joint, Task Force	

15.Abstract:

The purpose of this paper is to demonstrate how to apply conventional targeting techniques in sequencing and synchronizing the Operational Fires of Operational C2W. It proposes a methodology for applying the Decide portion of the Decide, Detect, Deliver, and Assess process used for targeting in the U.S. Army. It describes how the lethal and non-lethal fires of C2W can be applied at the operational level of war as Operational Fires. Further, it recommends giving the responsibility for planning and execution of C2W to the Joint Special Operations Task Force Commander on a permanent basis. These recommendations are designed to make the Joint Task Force Commander more comfortable with the employment of C2W and to increase the importance of C2W role in mission accomplishment.

16.Distribution / Availability of Abstract:	**Unclassified** X	**Same As Rpt**	**DTIC Users**
17.Abstract Security Classification: UNCLASSIFIED			
18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19.Telephone: 841-6461		**20.Office Symbol:** C	

Daniel A. Nolan III
LTC, USA
05/17/98

Targeting Command and Control Warfare as Operational Fires.

Introduction It is nearly impossible to pick up a professional journal today and not be assailed by yet another article touting the paradigm shattering effects of "leveraging information". The importance of Information Operations (IO) is evidenced by Department of Defense Directive S3600.1 Information Operations, wherein the information pie is divided amongst the DoD players. The Secretary defines IO as "Actions take to affect adversary information and information systems while defending one's own information, and information systems". The Chairman, Joint Chiefs of Staff is made responsible for, among other things, "Establishing doctrine to facilitate the integration of IO concepts into joint operations". The C,JCS has designated Command and Control Warfare (C^2W) as the purely military slice of IO.[1] Joint Doctrine for Command and Control Warfare, JP 3-13.1 further defines considerations for planning C^2W without providing the tactics, techniques and procedures (TTP) required to frame the problem. "Effective C^2W planning requires a *framework that focuses the battle staff*, thereby ensuring a plan that supports the commander's concept of operation by integrating the elements of C^2W into a coherent, synchronized plan."[2] With these words, U.S. Army doctrine in FM 6-100, Information Operations, lays out a service framework for thinking about Command and Control (C^2) attack. What is not described at any level in our doctrinal literature is a methodology for thinking about C^2 targeting at the operational level of war. The tendency to think about information operations in technological terms favors the high end of the spectrum of war, but IO is equally applicable along the continuum. The lack of TTP has lead operational

commanders to diminish the importance of Information Operations and relegate it to the "intel types" to sort out.

At the operational level of war C^2W can also serve the function of Operational Fires[3]. A discussion of Operational Fires is below. In this context Operational C^2W is employed so as to cause a decisive impact on the outcome of campaigns or major operations. The lethal and non-lethal tools in C^2W are an extension of Operational Fires.

In the execution of C^2W, the services all have as their ultimate objective an opposing information dependent process[4]. The ultimate information dependent process is decision-making and the ultimate node is the key enemy decision-maker. The purpose of C^2W as Operational Fires is to cause that decision-maker to be unable to reduce uncertainty in a timely manner, producing an endstate in which the enemy decision-maker is unable to gain information, cope with information, or unable to execute. This will have a decisive impact on the outcomes of major operations and campaigns if targeted properly. The pillars of C^2W, Electronic Warfare (EW), Psychological Operations (PSYOP), Deception, Operations Security (OPSEC) and Physical Destruction provide the means to this end. The targeting process links the means to the ends. As part of the targeting process we must identify the system or systems designed to protect that target. Just as Suppression of Enemy Air Defense provides freedom of action for Air Operations, we must be able to "suppress" information defensive systems to allow ourselves freedom of "Information Maneuver" without compromising the final attack. It is the operational sequencing and synchronization of these tools that give them their decisive impact. I define information maneuver as gaining temporal advantage over an opponent in order to

bring your information dominance to bear. The final aim of C^2W is to break the opposing decision-maker's decision cycle so that he never reaches the action phase or he chooses action that plays to our strength. **The purpose of this paper is to demonstrate how to apply conventional targeting techniques in sequencing and synchronizing the Operational Fires of Operational C^2W.**

I will use the U.S. Army targeting methodology described in FM 6-20-10, Tactics, Techniques, And Procedures For The Targeting Process , and adapt that system for Command and Control Warfare. The methodology in its most simple form is Decide, Detect, Deliver and Assess[5]. I will examine the Decide phase and show how the elements of C^2W must be employed in a sequenced and synchronized manner in order to achieve the desired effects on the target. This methodology supports the seven-step process discussed in Appendix C, FM 100-6, Information Operations.

The current literature does not fix the responsibility for targeting C^2W. One school of thought recommends a C^2W Cell for the planning and execution of IO. The other school focuses on the separate pillars and targets them, as they currently are, in accordance with doctrine using the Joint Targeting Coordination Board (JTCB). I will suggest another Joint Task Force element as the responsible agency.

Terms and Definitions As a preface for discussion a doctrinal basis is required in order to establish a common language for understanding C^2W. In the writings of Professor Milan Vego at the Naval War College, several useful concepts for thinking about the operational level of war may be found. One of these is the concept of Operational Fires. Operational Fires are those lethal and nonlethal fires that are planned

by operational commanders to have a decisive effect on major campaigns, utilizing forces not directly tactically engaged. The decisive effect is the ends sought. In the case of C^2W, at the operational level this is most often the disposition of enemy forces that support friendly operational goals. As mentioned earlier, C^2W, as a subset of Information Operations, is the military's role. The tools are deception, psychological operations, electronic warfare, operations security and physical destruction. These are the means to the end. The process that brings those means to bear to achieve the ends is the Targeting Process. The targeting process links the means to the ends. The operational commander must decide on the targets that will produce the desired decisive effect, detect those targets, deliver the proper tool in the proper sequence and assess the success or failure of the attack. I use the term "Information Maneuver" to emphasize the decisive effect of the information on the modern battlefield. Just as Suppression of Enemy Air Defense provides freedom of action for Air Operations, we must be able to "suppress" information defensive systems to allow ourselves freedom of "Information Maneuver" without compromising the final attack. It is the operational sequencing and synchronization of these tools that give them their decisive impact. In short, I define information maneuver as gaining temporal advantage over an opponent in order to bring your information dominance to bear. The final terms employed are the concepts of Operational Sequencing and Synchronization. This is the process of ensuring that the attack process produces a synergistic effect and is not counter productive. Planners must understand the 2^d and 3^{rd} order implications of attacks and make sure they are synchronized across the strategic, operational and tactical levels of war.

The Targeting Process The Decide, Detect, Deliver and Access process is analogous to the Observe, Orient, Decide and Act (OODA) loop. It describes a decision/action process. The Decide process begins with target value analysis (TVA). The first phase in TVA is templating the battlefield. Templating is the process of describing in two dimensions the time and space relationship of various elements of opposing forces' capabilities. For C^2W targeting, this will go beyond the normal doctrinal templating of an enemy's physical force and attempt to portray the information targets. CJCS MOP 30 describes the integrated intelligence support required for C^2W. There is no prescribed C^2W template. A C^2W template is required and should show C^2 nodes, key communications centers, sensors and a decision graphic of some sort that indicates the "targetability" of enemy decision-makers. This "targetability" would be a function of the level of decision on a hierarchical scale that the target could make (e.g., change in task organization or unit dispositions), the susceptibility of the decision-maker's systems to C^2 attack and a personality profile. This is described in C^2W Attack planning process as identifying how C^2-attack could support the overall mission and concept of operations[6].

Templating provides a visualization of the battlefield. The next step in TVA is to make the targeting relevant. In order to do this, a clear understanding of a concept or vision of a future state of events describing the disposition of the two forces relative to each other in time, space and circumstances is required. This is derived from the endstate as expressed in the Commander's intent. The C^2 attack template would be able to identify those targets that are capable of producing those circumstances. In the case of an opposing decision-maker, the circumstances can generally be described as an action or inaction, depending on the situation we wish to create. Targets may now be analyzed for

their likelihood of creating those circumstances. In C^2W the target is ultimately the opposing decision-maker or his support systems for decision. In order to evaluate people or systems as a potential target, several things must be considered. First, does the target have the ability to cause the circumstance to exist? This is a function of level of command, autonomy and doctrinal propensity to act. Next would be a determination of how the circumstances are to be created, through action or inaction. This is accomplished by considering how the target gathers, processes and acts upon information. The gathering and processing of information is about the same regardless of the level of technological sophistication. The process is a matter of the decision-maker deciding what is required to know about his opponent, gaining that information as facts or making assumptions where facts are not available and then acting on that information while it still has time-value. Whether using satellites or kids on the corner, a Sun Sparc or chicken innards, the process is about the same. What is important is the recognition of what types of systems are involved. The higher the level of technological sophistication, the greater the volume of information that can be gathered and the faster that information can be processed. Recognition of the level of technological sophistication is the most difficult portion of the TVA and will be most dependent on intelligence analysis. Intelligence support to this phase of planning is intense, however a database could be prepared ahead of time, much like the target sheets used for conventional targeting. This would be a very volatile database and require intense management if maintained on a regular basis. The alternative is a process of generating the database on an as needed basis given the need for contingency operations. If the target's action is required for the success of his operation, it qualifies as a high value target (HVT)[7]. HVTs are defined in this context as those

actions, knowledge or assets the *enemy decision-maker requires* for success. In C^2W, not all information systems qualify as HVT because they are not indispensable to the enemy's success. The key to understanding HVTs is considering at which level of war the operations are focused (tactical, operational or strategic) and how the target relates to the enemy's plan.

The next step is to determine if the HVT is a high payoff target (HPT)[8]. If the action or inaction by the target will produce a *significant advantage for friendly forces*, it qualifies as an HPT. HPTs also consider the degree of protection of the intended target and determines if the payoff is worth the investment. The benefit produced by attacking the target must be worth the cost. If a particular communications system is producing high quality intelligence, it's physical destruction as part of a larger plan might not produce a payoff commensurate with the cost of lost intelligence. Once the HPTs are determined, the "weaponeering" process can begin. Weaponeering is the process of determining the optimum system for application against the target. In C^2W, the weapons are the five pillars of deception, EW, PSYOPS, OPSEC and physical destruction. Which weapon is chosen is a function of the effect desired: action or inaction.

At this point it is worth discussing the Joint Vision 2010 concept of Information Superiority (IS). IS is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same[9]. In essence this means that friendly forces have absolute knowledge of the enemy and the enemy has no knowledge or has information that would cause him to act in a manner advantageous to friendly forces. The complete denial of information to an opposing

force is an admirable but not realistic goal. Being able to provide information that would cause him to act in a manner advantageous to friendly forces is the more likely case. This is the nature of deception.

If the intent is to cause the decision-maker to act, deception is the weapon of choice[10]. Deception provides information; the other pillars serve to deny information or support. If the intent is to cause inaction, then the weapon of choice is a function of the node to be attacked. Inaction can be cause by blocking information (EW), or denying information about yourself (OPSEC). Inaction may also result from perception manipulation (PSYOPS) or the ultimate inaction, physical destruction. The node for attack can be information gathering, process and/or decision dissemination. Each of these nodes will require analysis to determine their vulnerability to attack.

Another key consideration in weaponeering is to determine what systems protect the target. Just as air defense artillery protects infrastructure and units from air attack, a deception target is likely to be protected from information attack. These defenses take the form of encryption to preclude data attack, OPSEC to deny knowledge of intended actions, SIGSEC to reduce vulnerability to EW, etc.. The identification and defeat of these systems is of equal importance to the deception plan itself. A clumsy attempt at data attack will provide the enemy indicators of friendly intent before the final act. The true synchronization challenge lies is breaching the defense without tipping your hand. How this is accomplished is a function of the target and the defense systems, however, consideration of one's own OPSEC is of paramount importance. "When developing the concept of operation, it is important to recognize the potential for both mutual

reinforcement and mutual conflict among the five elements of C^2W." is how this is described in step six of C^2 attack planning[11]. This is the point at which planners must concern themselves with the concepts of operational sequencing and synchronizing. With deception as the key enabler, how the other pillars of C^2W are employed must provide mutual reinforcement. If the deception plan calls for the movement of forces, destroying the headquarters that is to issue the order or jamming the communications link that passes that order results in conflict and not reinforcement.

The deception plan must have as a minimum, a target, an intended outcome and a story intended to influence the targeted decision-maker to take action that causes the outcome. For C^2W to qualify as Operational fires that outcome must have a decisive effect on operations. The next step is the development of the story. The story is a function of the target's personal decision style and susceptibility to suggestion. This is the most creative process and requires superb intelligence concerning the decision-maker.

Once preliminary targeting for deception operations is developed, wargaming of alternative courses of action occurs, during which the scheme of maneuver and fires is developed. The scheme of information maneuver would likewise be developed at this time. Normally, the HPTs are then entered into an Attack Guidance Matrix (AGM) that spells out the target types, the acquisition means, the attack criteria and the means. In information maneuver, the plan of attack must be closely managed because of the intellectually fleeting nature of the targets. We cannot afford to wait for a sensor to detect a target, deliver against it and then assess damage. The key events and time in information maneuver are a function of the synchronized engagement by multiple means and the

amount of time required for the desired action (or inaction) to be detected. Currently there is no organization that functions in this manner, except for the Deep Operations Coordination Center (DOCC)[12] in U.S. Army Corps and Divisions. The DOCC plans and executes operations from the same staff element. The C^2W cell at all levels can perform the same function, but it must be closely integrated with the Operations element and the executors of the synchronized C^2W plan.

A Home for Command and Control Warfare Our current doctrine does not delineate the responsibility for planning and executing C^2W adequately. Targeting at the joint level is the responsibility of the Joint Forces Commander (JFC) who normally convenes a JTCB[13]. Joint Doctrine also calls for the formation of a C^2W cell as an additional planning staff. Responsibility for execution of C^2W IS left to the J3 to synchronize.[14] This requirement to further defuse a thin joint staff is likely to cause JFCs to be reluctant to form this organization. Tactics, techniques and procedures are required for the operations of the C^2W cell and the DOCC provides the blueprint.[15] Rather than form yet another staff element and give responsibility for execution to a staff officer, I recommend using the Joint Special Operations Task Force (JSOTF) Commander to perform this mission. His responsibilities span the other component commander (land, air and maritime), he is already responsible for psychological operations. If made the single focal point for planning of deception operations, the JSOTF would be able to sequence and synchronize the C^2W effort across the Joint Task force. The C^2W Cell would be placed under the JSOTF with coordination responsibilities to the JTCB. Rather than an ad hoc organization, the C^2W Cell should be a permanent part of the JSOTF staff. This would provide a single commander with responsibility for C^2W and eliminate the necessity

for reducing staff manning levels. A hotly debated topic in the IO world is the alternative to this concept. It calls for the formation of a Joint Forces Information Operations Task Force or JFIOTF. The JFIOTF would be responsible for all aspects of C^2W for the Joint Task Force and be at a command level commensurate with the other component commanders. Besides the obvious resource problem of redundant staffs, the JFC could have a potential span of control that exceeded his ability to manage. Imagine the JFMCC, JFACC, JFLCC, JSOTF, JPOTF, JCMOTF and now the JFIOTF all crowded around the Joint table. The potential for chaos is enormous.

Tactics, Techniques and Procedures The flow diagram at Appendix 1illustrates the methodology of the targeting process. It shows the transformation of a target from TVA to HVTs and into HPTs. TTP for the C^2W are still in the nascent stage of development. In general, JTCBs look at targeting efforts over a 72 to 96 hour period. The JSOTF could form a C^2W Cell that coordinated its planning and execution process with the JTCB. During the 72 to 96 hour time periods, operations would be either in the planning phase or execution phase by 24-hour periods. Each 24-hour period would be managed by a Battle Captain with an interdisciplinary team capable of planning and executing the operations for that period. Two targeting meetings are required daily. The first meeting is a decision briefing on the HPTs to be attacked 72 hours out. This meeting produces the C^2W focus for planning. The results of this decision briefing, the C^2W focus, is used to develop courses of action for wargaming. The second portion of this meeting is where the results of the wargaming are briefed and approval for attack plans to be executed 48 hours out is gained. The second meeting is used to gain final approval from the JFC for attacks to occur during the next 24 hour period. Any changes in the attack

plan and risk management are briefed at this time. The products of this meeting are the orders supporting C^2 attack. These targeting meetings would serve two general purposes. First is to focus the efforts of the JTF toward mutually supporting attacks based upon the commander's intent. The second purpose would be for providing a forum for coordination of the various attack means. Each stage of the planning and execution are closely coordinated with the higher headquarters as well as subordinates. The purpose of this coordination is to facilitate target handover as well as reduce redundancy in target attack. These mechanisms would well serve C^2W planning process and can be readily adapted. For an excellent discussion of the organization and operation of a Heavy Division Deep Operations Coordination Cell, see Field Artillery Journal, April 1995.

The Spectrum of Conflict This thought process or methodology for target development is as applicable in the deserts of Southwest Asia as they are in the market place in Mogadishu[16]. Thinking about information maneuver in terms of action or inaction, having the intelligence support required to assist in target value analysis and carefully considering the synergistic effects of the weapons of C^2W are challenges to be faced by all IO planners. The key is to develop a way of thinking about C^2 attack that leverages the existing doctrine against the tremendous force multipliers of the pillars of C^2W.

Conclusion C^2W has the potential to have a decisive effects on operations, using forces not directly tactically engaged, and planned by operational level commanders. Under these circumstances C^2W qualifies as operational fires. This framework will help the operational level commander understand the poetential impact of C^2W. It will also help to build trust in C^2W by couching it in a familiar methodology. By de-mystifying C^2W the

commander will become more comfortable in it's use. Right now, most operational commanders understand (and trust) a "smoking hole" better than a deceived opponent. The Decide, Detect, Deliver and Assess methodology described in FM 6-20-10 is readily adaptable to the C^2W targeting process and the six step process describe in FM 100-6 will help him understand how to employ it. If a C^2W cell is established permanently as part of the JSOTF and coordinates its efforts with the JTCB, the JFC will know where the planning and execution ought to be done and who will do it. If the JFC can understand what it is, why it is important, where it is done and by whom, then the only question left for him to answer is when: in any battlespace, from the low to the high end of the spectrum of conflict and at any level of war.

---

[1] Joint Chiefs of Staff, Joint Doctrine for Command and Control Warfare, (Joint Publication 3-13.1), 7 Feb 1997, pg. vi
[2] Department of the Army, Information Operations, (FM 100-6), Appendix C Washington, DC 27 Aug 1996*
[3] Milan Vego, On Operational Art (2d Draft), U.S. Naval War College, March 1998, pg. 156
[4] JP 3-13.1, pg. v
[5] Department of the Army, Tactics, Techniques, And Procedures For The Targeting Process, (FM 6-20-10) 08 MAY 1995*
[6] FM 100-6, Appendix C*
[7] FM 6-20-10, Appendix A, pg. A-8*
[8] ibid., pg. A-9
[9] Joint Chiefs of Staff, Joint Vision 2010, Joint Electronic Library, May 1997
[10] Joint Chiefs of Staff, Joint Doctrine for Military Deception, (JP 3-58), 31 May 1996, pg. II-1
[11] FM 100-6, Appendix C,*
[12] FM 6-20-10, Chap 3*
[13] Joint Chiefs of Staff, Doctrine for Joint Operations, (JP3-0), February 1995, pg. III-26
[14] JP 3-13.1, pg. IV-2
[15] FM 100-6, Appendix C,*
[16] JP 3-13.1, pg. V-6

*Electronic documents without page numbers

BIBLIOGRAPHY

U. S. Joint Chiefs of Staff, Doctrine for Joint Operations, (JP3-0), February 1995

U. S. Joint Chiefs of Staff, Joint Doctrine for Command and Control Warfare, (Joint Publication 3-13.1), 7 Feb 1997

U. S. Joint Chiefs of Staff, Joint Doctrine for Military Deception, (JP 3-58), 31 May 1996

U. S. Joint Chiefs of Staff, Joint Vision 2010, Joint Electronic Library, May 1997

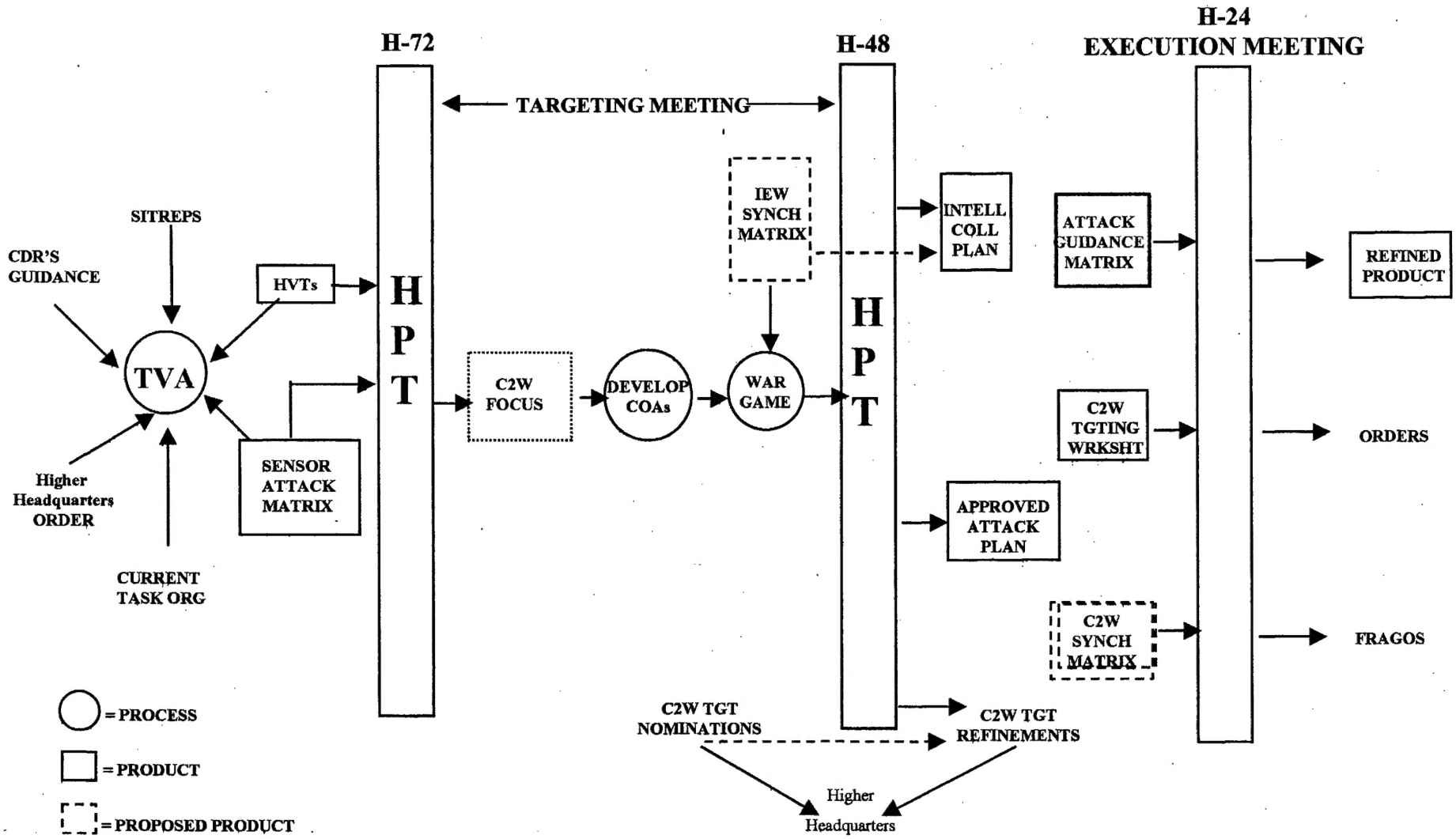
U. S. Department of the Army, Information Operations, (FM 100-6), Washington, DC 27 Aug 1996

U.S. Department of the Army, Tactics, Techniques, And Procedures For The Targeting Process, (FM 6-20-10) 08 MAY 1995

Vego, Milan On Operational Art (2d Draft), U.S. Naval War College, March 1998

Schwartau Winn, InfoWar.com, <http://www.infowar.com/>

C2 Target Flow Chart



Appendix 1